

REMOTE MONITOR SYSTEM

Patent Number: JP11161517

Publication date: 1999-06-18

Inventor(s): YAMAMOTO ATSUSHI

Applicant(s): MEIDENSHA CORP

Requested Patent: JP11161517

Application Number: JP19970325538 19971127

Priority Number(s):

IPC Classification: G06F11/30; G05B23/02; G06F9/06; G06F12/14

EC Classification:

Equivalents:

Abstract

PROBLEM TO BE SOLVED: To prevent infection with viruses and to prevent the loss of a monitoring function in the case of turning a personal computer to a central processing unit and monitoring and further controlling an equipment through an input/output device.

SOLUTION: In this system for connecting the central processing units 11 and 12 and the input/output devices 61 - 6N by 'Ethernet (R)', the central processing units 11 and 12 are provided with a performance monitoring application 5 for performing monitoring for the file size of the respective kinds of applications 2 and 3 and resources managed by an OS 4. The input/output devices 61 -6N are provided with an abnormality judgement function 12 for judging whether or not the central processing units are infected with the viruses from the data monitored by the performance monitoring application 5 and automatically executing a virus coping program to all the central processing units 11 and 12 at the time of judging that they are infected with the viruses.

Data supplied from the **esp@cenet** database - I2

(1) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-161517
(43) 公開日 平成11年(1999)6月18日

(5) (a) C1*	識別記号	F1
G 0 6 F	11/30	G 0 6 F
G 0 5 B	23/02	1/30 D
G 0 6 F	9/06	G 0 5 B 23/02 3 0 2 J
	12/14	G 0 6 F 9/06 5 5 0 Z
		12/14 3 1 0 Z

審査請求 未請求 請求項の数2

O.L. (全4頁)

(21) 出願番号 特願平9-325538

(71) 出願人 000006105

(22) 出願日 平成9年(1997)11月27日

(72) 発明者 山本 厚史

(74) 代理人 弁理士 志賀 富士弥 (外人名)

明鏡舎内

監視機能

【特許請求の範囲】

【請求項1】 パーソナルコンピュータを中心処理装置として、入出力装置を通して設備機器の監視さらには制御をする遠方監視システムにおいて、前記中央処理装置は、格納する各種アプリケーションのファイルサイズ及びOSが管理する資源について監視を行うパフォーマンス監視手段を設け、前記入出力装置は、前記パフォーマンス監視手段が監視するデータから中央処理装置が監視するデータに感染したか否かを判定し、ウイルスに対する対応プログラムを自動的に実行する異常判定手段を設けたことを特徴とする遠方監視システム。

【請求項2】 前記異常判定機能は、前記ウイルス対処プログラムの実行後もウイルス感染を判定したとき、前記中央処理装置が保存するデータの全てを外部媒體のデータで代替するデータを備えたことを特徴とする請求項1記載の遠方監視システム。

【請求項3】 遠方監視システムは、例えば変電所の監視には、所内各設備機器の子局から監視室側の親局に監視情報を伝送し、親局側の監視処理装置にて機器の状態等を監視する。前記機能も持つシステムでは、親局側から子局側に制御情報も伝送する。

【請求項4】 親局側の監視処理装置は、その性格上、コンピュータを中核部として構成され、コンピュータも技術の進歩シムシステムの大規模化に伴いミニコンピュータからメインフレーム、さらにワークステーションと進化し、現在では低価格化と高機能化されたパーソナルコンピュータを採用するものが淘汰できている。

【請求項5】 パーソナルコンピュータは、ネットワークの接続やワープロ・ゲームなど多種多様な目的に使用できるため、その内部データ破壊を目的としたウイルスプログラムとの接触の機会が多く、ウイルスプログラムと接触したときには重大な障害を受けてしまう。

【請求項6】 特に、パーソナルコンピュータが監視システムや監視制御システムの中核部とされる場合、ウイルスプログラムに感染すると、コンピュータ動作への干渉や設備の監視や制御が不能になるなど、深刻な事態になってしまう。

【請求項7】 ウィルスプログラムから直接接続するものとして、手動又はバッチファイル等を使って市販のウイルス対処プログラムを実行させる方法が採られている。

【請求項8】 ワイヤレスLAN装置から監視機能が監視するデータから中央処理装置がウイルスに感染したか否かを判定し、ウイルスに感染したと判定したときの中央処理装置に対してウイルス対処プログラムを自動的に実行する異常判定機能1.2を設ける。

【請求項9】 本発明は、ウイルス感染による不具合の深刻な結果となってしまう。

【請求項10】 本発明の目的は、ウイルス感染及び不具合の免疫を自動的に検知及び対処処理できる遠方監視システムを提供することにある。

(2) (0007)

【発明の解決しようとする課題】 従来のウイルス対処方法では、ウイルスプログラムを実行することになる。

(0008) このため、監視室の運転員がウイルス感染によって対応する事ができないが、夜間など、人のないときにウイルスによる不具合が発生したときには対応が遅れ、監視機能の喪失などシステムに深刻な結果となってしまう。

(0009) 本発明の目的は、ウイルス感染及び不具合の免疫を自動的に検知及び対処処理できる遠方監視システムを提供することにある。

(0010) 【概要】 本発明は、ウイルス感染の判定機能を設け、処理装置がウイルス感染したときにウイルス対処プログラムを自動的に実行するようしたるもので、以下の構成を持つ。

(0011) パーソナルコンピュータを中心処理装置とし、入出力装置を通して設備機器の監視さらには制御を行う遠方監視システムにおいて、前記中央処理装置は、格納する各種アプリケーションのファイルサイズ及びOSが監視する資源について監視を行ラバフォーマンス監視手段を設け、前記入出力装置は、前記パフォーマンス監視手段を監視するデータから中央処理装置がウイルスに感染したか否かを判定し、ウイルス対処装置に於いて、前記中央処理装置に対する異常判定手段を設けたこととした。

(0012) また、前記異常判定機能は、前記ウイルス対処プログラムの実行後もウイルス感染を判定したとき、前記中央処理装置が保存するデータの全てを外部媒体のデータで代替するデータを備えたことを特徴とする。

(0013) 【発明の実施の形態】 図1は、本発明の実施形態を示す監視システム構成である。監視システムの中央処理装置1.1、1.2は、パーソナルコンピュータで構成される。

【実施形態のシステム構成】

The diagram illustrates the internal components of a personal computer system. At the top is the CPU, which is connected to RAM and ROM. Below the CPU is the HDD. To the right of the CPU is a keyboard and a mouse. To the left is a monitor. Below the monitor is a NIC, which is connected to a LAN. A PSU is at the bottom left, connected to the system via a power cord.

(0014) パフォーマンス監視アリケーション5は、OS4と通信を行い、パーソナルコンピュータにインストール(搭載)されている各種アリケーション3.4のファイルサイズをデータベースとして保持する。また、アリケーション5は、OS4と通信を行い、パーソナルコンピュータ内の資源について監視を行う。

(0015) 入出力装置6～6nは、出入力装置6～6nは、イーサネット等を介して接続される。これらは、監視システムの中央処理装置1.1、1.2と入出力装置6～6nを介して接続される。

【0016】 これより入出力装置6～6nは、直後に又は子局を介す。

【0017】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0018】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0019】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0020】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0021】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0022】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0023】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0024】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0025】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0026】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0027】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0028】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0029】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0030】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0031】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0032】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0033】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0034】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0035】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0036】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0037】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0038】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0039】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0040】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0041】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0042】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0043】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0044】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0045】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0046】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0047】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0048】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0049】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0050】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0051】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0052】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0053】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0054】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0055】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0056】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0057】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0058】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0059】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0060】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0061】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0062】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0063】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0064】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0065】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0066】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0067】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0068】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0069】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0070】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0071】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0072】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0073】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0074】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0075】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0076】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0077】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0078】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0079】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0080】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0081】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0082】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0083】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0084】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0085】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0086】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0087】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0088】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0089】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0090】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0091】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0092】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0093】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0094】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0095】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0096】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0097】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0098】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0099】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0100】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0101】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0102】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0103】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0104】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0105】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0106】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0107】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0108】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0109】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0110】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0111】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0112】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0113】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう。

【0114】 本発明の特徴は、ウイルス感染による不具合の深刻な結果となってしまう

して監視対象又は監視制御対象となる各種の設備機器7
～7₄、8～8₃の状態信号の取り込み及び制御信号の
出力を行い、中央処理装置1、1₂との間で情報授受を
行う。

[00116] 入出力装置6～6₃のアプリケーション構
成は、装置6に代表して示すように、アプリケーショ
ンとして設備機器との入出力処理機能9、データ保存機
能10及び通信機能11の他に、CPU異常判定機能1
2を備える。

[00117] この異常判定機能1₂は、中央処理装置1
～1₂のパフォーマンス監視アプリケーション5との間
で通信を行い、アプリケーション5から取り込んだデー
タについてそのファイルサイズや資源の変化から
ウイルスに感染したか否かを判定し、ウイルスに感染し
たと判定したときは中央処理装置1、1₂に対してウ
イルス対処プログラムを実行する。

[00118] このプログラムの実行は、例えば、中央処
理装置1がウイルスに感染したと判定したときに該裝
置1に対してウイルス対処プログラムを実行すると
に、既りの中央処理装置1に対してもウイルス対処ブロ
ログラムを実行する。

[00119] したがって、本実施形態によれば、中央処
理装置1、1₂の少なくとも1台がウイルス感染したこ
とを入出力装置6～6₃の1つが判定したときに直ちに
全ての中央処理装置1に対して自動的にウイルス対処ブロ
ログラムを実行する。

[00200] これにより、ウイルス感染を早期に判定

し、設備機器の監視不能などの発症前にウイルス感染に
対応できる。また、1台の中央処理装置のウイルス感染
を全ての中央処理装置に対してウイルス対処プログラム
を実行するため、他の健全な中央処理装置がウイルスに
感染する前に対処できる。

[00201] なお、ウイルス対処プログラムの実行後、
CPU異常判定機能1₂が再度ウイルス感染を検知した

ときは、中央処理装置内のすべてのデータを更新するこ
とで監視機能の確保を確実にことができる。

[00221] 例えば、図2に示すように、中央処理装置
1₁がウイルス感染し、入出力装置6₁がウイルス対処ブ
ログラムを実行した後もCPU異常判定機能1₂がウイ
ルス感染を検知したとき、中央処理装置1₁に接続され
た外部媒体1₃に対して代替え指令を発生し、中央処理
装置1₁内のハードディスクの全てのデータファイルを
健全なものに替える。

[00231] [発明の効果] 以上のように、本発明によれば、ウイル
ス感染の判定機能を設け、処理装置がウイルス感染した
ときに直ちにウイルス対処プログラムを自動的に実行す
るようにしておいたため、ウイルス感染の自動検知及び発症前
にウイルス対処プログラムの実行ができる、夜間など人の
いないときにウイルスに感染するも監視機能の確保を確
実にすることができる。

[図面の簡単な説明]

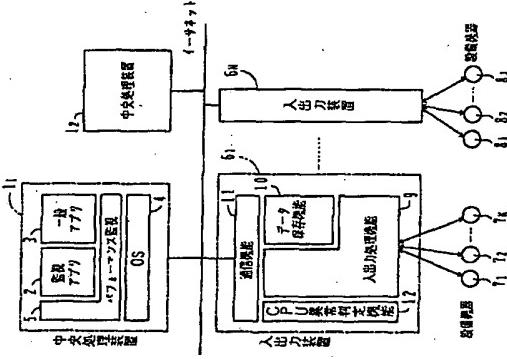
[図1] 本発明の実施形態を示すシステム構成図。
[図2] 実施形態におけるデータ替え処理。

[符号の説明]

- 1～1₂…パーソナルコンピュータ構成の中央処理装置
- 2…監視アプリケーション
- 3…一般アプリケーション
- 4～O_S
- 5…パフォーマンス監視アプリケーション
- 6～6_N…出力装置
- 7～7_N、8～8_N…設備機器
- 9…入出力処理機能
- 10…データ保存機能
- 11…通信機能
- 12…CPU異常判定機能
- 13…外部媒体

[図1]

実施形態のシステム構成



[図2]

実施形態のデータ替え処理

